

**METHOD OF AND APPARATUS FOR FILTERING ACCESS, AND  
COMPUTER PRODUCT**

FIELD OF THE INVENTION

5           The present invention relates to a technology for allowing only a correct access request to pass from clients to a server that provides services in response to access requests.

10   BACKGROUND OF THE INVENTION

          In recent years, with the development in network technique, the use of WWW (WorldWide Web) serving as a dispersion system on the Internet has rapidly spread, and various HTTP servers for providing various services in response to various requests (access requests) from clients are accumulated. However, with the accumulation of the servers, incorrect accesses to servers by clients gradually increase in number.

          More specifically, intruders or attackers incorrectly use servers of companies, associations, individuals, and the like without any authority, obstruct operations, or break (clutch) the servers, so that incorrect accesses in which persons who use the servers intentionally perform acts except for acts allowed by authorities given to the persons increase in number. For this reason, the necessity that the

reliabilities of servers are secured by refusing incorrect accesses to the servers have intensified.

Conventionally, in order to protect a server from an incorrect access by a client, a fire wall is generally  
5 structured between the Internet and a corporate LAN (Local Area Network).

The fire wall is software for preventing external intrusion on a computer or a network connected to the Internet. A computer for fire wall which is designed to pass only  
10 specific data or specific protocols is set between a corporate LAN and the Internet, all data exchanges between the LAN and external computers are performed through this machine to prevent external intrusion.

In addition, in relation to the fire wall, incorrect  
15 access detection methods on network base and host base are known. The former, i.e., the incorrect access detection method on network base monitors a live packet flowing in a network to detect an incorrect access. The later, i.e., the incorrect access detection method on host base monitors  
20 log histories stored in a host to detect an incorrect access.

The transmission source client of an incorrect access is found out on the basis of an incorrect access detected by such an incorrect detection method, and transmission source information such as the IP address of the client who  
25 performs this incorrect access is accumulated in the computer

for fire wall. In this manner, it is generally performed that the fire wall refuses an access request from the client including the transmission source information as an incorrect access.

5           However, in the prior art described above, a client who performs an incorrect access in the past is recognized as an incorrect client, and an access request from the incorrect client is refused as an incorrect access. For this reason, although a server can controlled for an  
10 incorrect access from the client who is recognized as an incorrect client, the server cannot be controlled for an incorrect access from a client who is not recognized as an incorrect client. More specifically, the server cannot be controlled for the first incorrect access from a client which  
15 has not been recognized as an incorrect client.

For this reason, it is a very important problem to control a server for an incorrect access from a client which is not recognized as an incorrect client. Preferably, a framework which decides whether an access request is a  
20 correct access request or an incorrect access request without considering transmission source information of an access request is necessary.

#### SUMMARY OF THE INVENTION

25           It is an object of this invention to provide a filtering

apparatus which can prevent a server from an incorrect access from a client which is not recognized as an incorrect client. It is another object of this invention to provide a filtering method to be executed on the filtering apparatus according to the present invention. It is another object of this invention to provide a computer program which realizes the filtering method according to the present invention on a computer.

According to the present invention, an incorrect request database stores patterns of incorrect accesses to the Web server. Correctness of an access request from a client device to a server is estimated based on the patterns stored in the incorrect request database and a predetermined estimation rule. Decision about whether the access request is to be passed to the Web server is made based on the result of estimation on correctness of an access request and a predetermined decision rule.

Other objects and features of this invention will become apparent from the following description with reference to the accompanying drawings.

#### BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram showing the configuration of a client server system according to a first embodiment.

Fig. 2 is a table showing a configuration of information

stored in an incorrect request DB.

Fig. 3 is a flow chart for explaining a procedure of a filtering process according to the first embodiment.

Fig. 4 is a flow chart for explaining a procedure of  
5 a filtering process according to a second embodiment.

Fig. 5 is a block diagram showing the configuration of a client server system according to a third embodiment.

Fig. 6 is a flow chart for explaining a procedure of a filtering process according to the third embodiment.

10

#### DESCRIPTION OF THE PREFERRED EMBODIMENTS

Embodiments of a filtering apparatus, a filtering method, and a computer program for causing a computer to execute the method according to the present invention will  
15 be described in detail below with reference to the accompanying drawings. In first to third embodiments described below, a case in which a filtering technique according to the present invention is applied to a server device for providing services depending on HTTP (HyperText  
20 Transfer Protocol) requests from a client device will be described below.

As a first embodiment, a case in which it is decided, by checking whether an HTTP request from a client device corresponds to the pattern of an incorrect request, whether  
25 an access is an incorrect access or not will be described

below.

(1) Entire Configuration of System

First, the configuration of a client server system according to the first embodiment will be described below.

5 Fig. 1 is a block diagram showing the configuration of a client server system according to the first embodiment. As shown in Fig. 1, the client server system according to the first embodiment has a configuration in which a plurality of client device 10 each having a Web browser 11, and a server  
10 device 20 having a request filter 30 serving as a filtering device and a Web server 40 are connected to each other through a network 1 such as the Internet such that the respective components can be communicated with each other.

Briefly, in this client server system, the client  
15 device 10 performs various process requests such as HTTP request to the server device 20 by the browser 11, and the Web server 40 of the server device 20 provides a service depending on an HTTP request from the client device 10 to the client device 10. The request filter 30 of the server  
20 device 20 is interposed between the client device 10 and the Web server 40, so that only a correct request of HTTP requests from the client device 10 is given to the Web server 40.

The client server system according to the first  
25 embodiment is characterized by a filtering process performed

by the request filter 30 of the server device 20. More specifically, the estimation unit 32 of the request filter 30 estimates that an access is an incorrect access when an HTTP request from the client device 10 corresponds to any one of the patterns of incorrect accesses stored in the incorrect request DB 33, and the decision unit 34 decides that the HTTP request which is estimated as an incorrect access by the estimation unit 32 is not given to the Web server 40, so that only the HTTP request can be given to the Web server 40 without considering transmission source information of the HTTP request.

## (2) Configuration of Client Device

The configuration of the client device 10 shown in Fig. 1 will be described below. With reference to Fig. 1, the client device 10 comprises the Web browser 11, basically performs a process request such as an HTTP request to the server device 20, interprets Web data provided by the Web server 40 of the server device 20, and performs display control (browse process) for displaying the data on an output unit such as a monitor or the like.

The client device 10 is also a device which can perform an incorrect access to the server device 20 depending on a malicious using method. More specifically, when the client device 10 is used by a user such as an intruder or an attacker with malice, such an incorrect access that the

user sees a password file on the Web server 40 which must be seen by a remote user, that the user requests a file which does not exist on the Web server 40 to stop the function of the Web server 40, or that the user executes an arbitrary  
5 system command on the Web server 40 by a request including a command letter string can be performed. The request filter 30 functions to protect the Web server 40 from an incorrect access by the client device 10.

The client device 10 can be realized by a mobile  
10 communication terminal such as a personal computer or a workstation, a home video game, an internet TV, a PDA (Personal Digital Assistant), or a mobile telephone set or a PHS (Personal Handy Phone System). In addition, the client device 10 is connected to a network 1 through a communication  
15 device such as a modem, a TA, or a router and a telephone line or a leased line, and can access the server device 20 according to a predetermined communication protocol (e.g., a TCP/IP internet protocol).

### (3) Configuration of Web Server in Server Device

20 The configuration of the Web server 40 in the server device 20 shown in Fig. 1 will be described below. As shown in Fig. 1, the Web server 40 of the server device 20 receives an HTTP request from the client device 10 through the request filter 20, and provides a service or the like for transmitting  
25 various pieces of information described in a markup language

such as an HTML (Hypertext Markup Language) to the client device 10 according to the HTTP request.

The Web server 40 performs the same operation as that of a general Web server in a functional concept. However, the Web server 40 mentioned here, unlike a general Web server, does not monitor a TCP (Transmission Control Protocol) of port number 80 assigned to the HTTP request in the server device 20.

More specifically, the HTTP request from the client device 10 is not directly received by the Web server 40, the request filter 30 receives the HTTP request to perform inter-process communication, so that only a correct HTTP request is given to the Web server 40.

#### (4) Configuration of Request Filter in Server Device

The configuration of the request filter 30 in the server device 20 shown in Fig. 1 will be described below. As shown in Fig. 1, the request filter 30 comprises a receiving unit 31, an estimation unit 32, an incorrect request DB 33, a decision unit 34, a transmission unit 35, a log management unit 36, an external notification unit 37, an external information acquiring unit 38, and an updating unit 39.

Of these components, the receiving unit 31 is a process unit for monitoring a TCP port of port number 80 in the server device 20 to receive an HTTP request from the client device 10 before the HTTP request is received by the Web server

40. The HTTP request received by the receiving unit 31 from the client device 10 is output to the estimation unit 32 and the transmission unit 33.

The estimation unit 32 is a process unit for estimating  
5 the correctness of the HTTP request on the basis of the patterns of incorrect accesses stored in the incorrect request DB 33 and a predetermined estimation rule 32a to output the estimation result to the decision unit 34.

The incorrect request DB 33 to which the estimation  
10 unit 32 refers in estimation will be described below. Fig. 2 is a table showing a configuration of information stored in the incorrect request DB 33. As shown in Fig. 2, the incorrect request DB 33 is a database in which the patterns of incorrect accesses to the server, and stores a plurality  
15 of patterns obtained by describing incorrect accesses collected in the network world by using an illustrated formal language.

For example, the pattern "URL = < //" shown in Fig. 2 means an incorrect request in which the start of a URL  
20 (Uniform Resource Locator) is "//", and the pattern of "CGI = phf, ARG = <Qname = root%OA" means an incorrect request in which a CGI (common Gateway Interface) name is "phf" and the start of an argument of the CGI is "Qname = root%OA". The pattern of "URL <>.. ¥.. ¥.. ¥.." means an incorrect  
25 request in which a URL includes "..¥..¥..¥", and the pattern

of "CGI>=. htr" means an incorrect request in which the end of a CGI name is ".htr".

Although not shown in Fig. 2, in the incorrect request DB 33, a plurality of incorrect command character strings for executing arbitrary system commands on the Web server 40 are stored. When the patterns of the command character strings are stored, the Web server 40 can be controlled for not only an incorrect access the attack method of which is known but also an incorrect access the attack method of which is not known.

With reference to the incorrect request DB 33, the estimation unit 32 estimates the correctness of an HTTP request on the basis of a predetermined estimation rule 32a. More specifically, when the HTTP request corresponds to any one of the patterns of incorrect accesses stored in the incorrect request DB 33, and estimates that the HTTP request is an incorrect access. On the other hand, when the HTTP request does not correspond to any one of the patterns of incorrect accesses stored in the incorrect request DB 33, the estimation unit 32 estimates that the HTTP request is a correct access.

Returning to the description of Fig. 1, the decision unit 34 is a process unit for deciding, on the basis of the estimation result received from the estimation unit 32 and the predetermined decision rule 34a, whether the HTTP request

is given to the Web server 40 or not to output the decision result to the transmission unit 35. More specifically, when the decision unit 34 receives an estimation result that the HTTP request is an incorrect access from the estimation unit 5 32, the decision unit 34 decides that the HTTP request is not given to the Web server 40 (impossible decision). On the other hand, when the decision unit 34 receives an estimation result that the HTTP request is a correct access, the decision unit 34 decides that the HTTP request is given 10 to the Web server 40 (possible decision).

The transmission unit 35 is a process unit for controlling transmission of the HTTP request received from the receiving unit 31 on the basis of the decision result received from the decision unit 34. More specifically, when 15 a possible decision is received from the decision unit 34, the HTTP request is given to the Web server 40 by inter-process communication. On the other hand, when an impossible decision is received from the decision unit 34, giving the HTTP request to the Web server 40 is refused, and the incorrect 20 request is wasted.

The log management unit 36 is a process unit for storing information related to the incorrect request which is decided not to be given to the Web server 40 by the decision unit 34 in the storage medium 36b and managing the information 25 on the basis of the predetermined management rule 36a. More

specifically, on the basis of the management rule 36a, pieces of information related to the incorrect request such as the contents of the incorrect request, transmission source information (IP address or host name), transmission time, the reason of an estimation result obtained by the estimation unit 32, and the reason of a decision result obtained by the decision unit 34 are selectively edited, and the selectively edited pieces of information are selectively stored in the storage medium 36b depending on the level of aggression of the incorrect request. For example, only incorrect requests having high levels of aggression are stored.

The pieces of information stored in the storage medium 36b can be output to the outside of the server device 20 by ejecting the storage medium 36b or using a communication line. In addition, the pieces of information stored in the storage medium 36b are analyzed to analyze the tendency of an incorrect access, so that a further countermeasure for maintenance of the Web server 40 can be performed.

The external notification unit 37 is a process unit for notifying information related to an incorrect request which is decided not to be given to the Web server 40 by the decision unit 34 to the external device 50. More specifically, as in the process performed by the log management unit 36, on the basis of the notification rule

37a, pieces of information related to the incorrect request such as the contents of the incorrect request, transmission source information (IP address or host name), transmission time, the reason of an estimation result obtained by the estimation unit 32, and the reason of a decision result obtained by the decision unit 34 are selectively edited, and the selectively edited pieces of information are selectively stored in the external device 50 depending on the level of aggression of the incorrect request.

10           The external device 50 which receives a notice from the external information acquiring unit 38 is a communication device which is operated by an administrator of the Web server 40, an administrator of the request filter 30, an administrator of the entire server device 20, an administrator of a public association (management center) which monitors the network as a whole, and the like (these administrators are generally called an "administrator"). The external notification unit 37, for example, rapidly notifies incorrect requests having high levels of aggression to the administrator on real time, and notifies incorrect requests having low levels of aggression to the administrator at once, so that the external notification unit 37 can urge the administrator which receives the notice to rapidly perform a countermeasure for maintenance of the Web server 40.

The external information acquiring unit 38 is a process unit for actively or passively acquiring, on the basis of the predetermined acquisition rule a, information used in an updating process performed by the updating unit 39 from the outside of the request filter 30 such as the external device 50 or the Web server 40. For example, the pattern of an incorrect request newly input by an administrator through the external device 50, change designation information of the estimation rule 32a input by the administrator through the external device 50, and the like are acquired, and information such as the status of damage or the contents of an incorrect request is acquired from the Web server 40 damaged by the incorrect request. The acquisition rule 38a is a rule which acquires only information from an authorized administrator.

The updating unit 39 is a process unit for updating, on the basis of the predetermined updating rule 39a, the incorrect request DB 33, the estimation rule 32a, the decision rule 34a, the management rule 36a, the notification rule 37a, the acquisition rule 38a, or information stored in the updating rule. For example, when the pattern of a new incorrect request is accepted from the external information acquiring unit 38, the pattern of the incorrect request is stored in the incorrect request DB 33. When change designation information of the estimation rule 32a is

accepted, the estimation rule 32a is changed depending on the change designation information. When the updating process is performed as described above, the updating unit 39 can tactfully cope with incorrect accesses advancing  
5 everyday.

#### (5) Filtering Process

A procedure of a filtering process according to the first embodiment will be described below. Fig. 3 is a flow chart for explaining the procedure of a filtering process  
10 according to the first embodiment. As shown in Fig. 3, the receiving unit 31 of the request filter 30 in the server device 20 receives an HTTP request from the client device 10 before the HTTP request is received by the Web server 40 (step S301).

15 The estimation unit 32 of the request filter 30 estimates the correctness of the HTTP request on the basis of the pattern of an incorrect access stored in the incorrect request DB 33 and the predetermined estimation rule 32a (step S302). More specifically, when the HTTP request  
20 corresponds to any one of the patterns of incorrect accesses, the estimation unit 32 estimates that the HTTP request is an incorrect request. On the other hand, when the HTTP request does not corresponds to any one of the patterns of incorrect accesses, the estimation unit 32 estimates that  
25 the HTTP request is a correct request.

Thereafter, the decision unit 34 of the request filter 30 decides, on the basis of the estimation result received from the estimation unit 32 and the predetermined decision rule 34a, whether the HTTP request is given to the Web server 40 or not (step S303). More specifically, the decision unit 34 decides whether it is estimated or not by the estimation unit 32 that the HTTP request is a correct request.

If it is decided by this decision that it is estimated that the HTTP request is a correct request (YES in step S303), the transmission unit 35 of the request filter 30 gives the HTTP request to the Web server 40 by inter-process communication (step S304), and the Web server 40 performs a process in a correctness decision state, e.g., a process of transmitting information depending on the HTTP request to the client device 10 (step S305).

In contrast to this, if it is decided that it is estimated that the HTTP request is an incorrect request (NO in step S303), the transmission unit 35 refuses to give the HTTP request to the Web server 40 (step S306), and the respective components of the request filter 30 perform processes in an incorrect decision state such as waste of an incorrect request, storage in the storage medium 36b, and notification to the external device 50 (step S307).

As has been described above, according to the first embodiment, without transmission source information of an



More specifically, the number of patterns, which correspond to the HTTP request, of the patterns of incorrect accesses is calculated, or the degrees of danger are given to the respective patterns to calculate the degrees of danger of the patterns which correspond to the HTTP request, so that an estimation value called a DI (Danger Index) representing the degree of danger of the HTTP request is calculated. The estimation value DI is an integer value falling within the range of, e.g., 1 to 100, and is calculated as a large value when the degree of danger of an HTTP request is high.

The decision unit 34 in second embodiment compares the estimation value DI calculated by the estimation unit 32 with a predetermined threshold value to decide whether the decision result is given to the Web server 40 or not, and outputs decision result to the transmission unit 35.

More specifically, if it is assumed that the predetermined threshold value is 50, when an estimation value the DI of which is 50 or more is received from the estimation unit 32, it is decided that an HTTP request is not given

to the Web server 40 (impossible decision). On the other hand, when an estimation value the DI of which is smaller than 50 is received from the estimation unit 32, it is decided that an HTTP request is given to the Web server 40 (possible  
5 decision).

A procedure of a filtering process according to the second embodiment will be described below. Fig. 4 is a flow chart for explaining the procedure of a filtering process according to the second embodiment. As shown in Fig. 4,  
10 the receiving unit 31 of the request filter 30 in the server device 20 receives an HTTP request from the client device 10 before the HTTP request is received by the Web server 40 (step S401).

The estimation unit 32 of the request filter 30  
15 calculates an estimation value DI depending on the degree of correspondence between an HTTP request and the patterns of incorrect accesses stored in the incorrect request DB 33 (step S402). The decision unit 34 of the request filter 30 compares the estimation value DI calculated by the  
20 estimation unit 32 with a predetermined threshold value to decide whether the HTTP request is given to the Web server 40 or not (step S403). More specifically, it is decided whether the estimation value DI is equal to or more than the threshold value or not.

25 If it is decided by the above decision that the

estimation value DI is smaller than the predetermined threshold value (YES in step S403), the transmission unit 35 of the request filter 30 gives the HTTP request to the Web server 40 by inter-process communication (step S404), and the Web server 40 performs a process in a correctness decision state, e.g., a process of transmitting information depending on the HTTP request to the client device 10 (step S405).

In contrast to this, if it is decided that the estimation value DI is the predetermined threshold value or more (NO in step S403), the transmission unit 35 of the request filter 30 refuses to give the HTTP request to the Web server 40 (step S406), and the respective components of the request filter 30 perform processes in an incorrect decision state such as waste of an incorrect request, storage in the storage medium 36b, and notification to the external device 50 (step S407).

As has been described above, according to the second embodiment, by comparison between an estimation value and a threshold value, it can be decided with some margin whether an access is an incorrect access or not. In this manner, the Web server 40 can be controlled with some margin for an incorrect access from the client device 10 which is not recognized as an incorrect client.

In the first and second embodiments, the case in which

estimation based on the patterns of incorrect accesses is performed for all HTTP requests from client devices is performed. However, the present invention is not limited to this case. The present invention can similarly applied  
5 to the case in which estimation is performed for only some of the HTTP requests.

As a third embodiment, a case in which filtering process constituted by two layers, and estimation based on the patterns of incorrect accesses is performed to some of the  
10 HTTP requests will be described below.

Fig. 5 is a block diagram showing the configuration of a client server system according to the third embodiment. The same reference numerals as in Fig. 1 denote the same parts in Fig. 5, and a description thereof will be omitted.  
15 An advance decision unit 71 and a correct request DB 72 which are characteristic parts of third embodiment will be described below.

The advance decision unit 71 of a request filter 70 in a server device 60 is a process unit for deciding whether  
20 estimation of an HTTP request can be omitted or not on the basis of the patterns of correct accesses stored in the correct request DB 72 and a predetermined advance decision rule 71a before estimation of correctness is performed by the estimation unit 32.

25 The correct request DB 72 which is referred to by the

advance decision unit 71 in decision will be described below.  
The correct request DB 72 is a database in which the patterns  
of correct accesses to the Web server 40. More specifically,  
the path of a file, which may be seen by a remote user, of  
5 files existing on the Web server 40 is stored.

The file which may be seen by the remote user is a  
file except for a file such as a password file which must  
not be seen by the remote user. For example, the file  
includes a file, such as an image file having a very high  
10 rate as request contents of an HTTP request to the Web server  
40, which is rarely incorrectly accessed.

With reference to the correct request DB 72, the advance  
decision unit 71 decides, on the basis of the predetermined  
advance decision rule 71a, whether estimation of the HTTP  
15 request can be omitted or not. More specifically, when the  
HTTP request corresponds to any one of the patterns of correct  
access, it is decided that estimation of the HTTP request  
can be omitted. On the other hand, when the HTTP request  
corresponds to any one of the patterns of correct accesses  
20 stored in the correct request DB 72, it is decided that the  
estimation of the HTTP request can be omitted.

The advance decision unit 71 outputs only the HTTP  
request the estimation of which cannot be omitted to the  
estimation unit 32, and omits the processes performed by  
25 the estimation unit 32 and the decision unit 34 with respect

to an HTTP request the estimation of which can be omitted to give the HTTP request to the Web server 40 through the transmission unit 35.

The patterns of correct accesses stored in the correct request DB 72 are updated by the updating unit 39 depending on a case in which an image file is added to the Web server 40.

A procedure of a filtering process according to the third embodiment will be described below. Fig. 6 is a flow chart for explaining the procedure of the filtering process according to this embodiment. As shown in Fig. 6, the receiving unit 31 of the request filter 70 in the server device 60 receives an HTTP request from the client device 10 before the HTTP request is received by the Web server 40 (step S601).

The advance decision unit 71 of the request filter 70 decides, on the basis of the patterns of incorrect accesses stored in the correct request DB 72 and the predetermined advance decision rule 71a, whether estimation of the HTTP request can be omitted or not (step S602). More specifically, the advance decision unit 71 decides whether the HTTP request corresponds to any one of the patterns of correct accesses stored in the correct request DB 72.

If it is decided by the above decision that the HTTP request corresponds to any one of the patterns of correct

accesses (YES in step S602), estimation of the correctness of the HTTP request is omitted, and the transmission unit 35 of the request filter 70 gives the HTTP request to the Web server 40 through inter-process communication (step 5 S605), and the Web server 40 performs a process in a correct decision state such as a process of transmitting information depending on the HTTP request to the client device 10 (step S606).

In contrast to this, it is decided that the HTTP request 10 does not correspond to any one of the patterns of correct accesses (NO in step S602), and the HTTP request is given to the estimation unit 32, and the same process as the filtering process in first and second embodiments is performed (steps S603 to 608).

15 More specifically, the estimation unit 32 of the request filter 70 estimates the correctness of the HTTP request (step S603), and the decision unit 34 decides whether the HTTP request is given to the Web server 40 (step S604).

If it is decided by the above decision that it is 20 estimated that the HTTP request is a correct request (YES in step S604), the transmission unit 35 of the request filter 70 gives the HTTP request to the Web server 40 by inter-process communication (step S605), and the Web server 40 performs a process in a correct decision state such as a process of 25 transmitting information depending on the HTTP request to

the client device 10 (step S606).

In contrast to this, if it is decided that it is estimated that the HTTP request is an incorrect request (NO in step S604), the transmission unit 35 of the request filter 70 refuses to give the HTTP request to the Web server 40 (step S607), and the respective components of the request filter 70 perform processes in an incorrect decision state such as waste of an incorrect request, storage in the storage medium 36b, and notification to the external device 50 (step S608).

As described above, according to the third embodiment, with respect to an HTTP request, such as an HTTP request having a high rate of request but a low level of aggression, for requesting an image file, a rapid process can be performed without the processes performed by the estimation unit 32 and the incorrect request DB 33. With respect to an HTTP request, having a high level of aggression, for requesting a password file or a file existing on the Web server 40, the processes by the estimation unit 32 and the incorrect request DB 33 are performed, so that the attack can be effectively prevented.

In the first to third embodiments, the case in which an HTTP request from the client device 10 is filtered is described. The present invention is not limited to this case, and can similarly applied to a case in which any

information such as FTP (File Transfer Protocol), telenet, or console which is input from the client device 10 to the Web server 40.

In the first to third embodiments, the case in which the request filters 30 and 70 serving as filtering devices are arranged in the server devices 40 and 60, respectively is described. However, the present invention is not limited to the case. For example, the present invention can similarly applied to any system configuration in which a request filter is interposed between a client device and a Web server such as a configuration in which request filters are arranged on the client device sides or a configuration in which a plurality of Web servers are controlled by one request filter.

The filtering methods described in the first to third embodiments can be realized by executing prepared programs in computers such as personal computers and workstations. The programs can be distributed through networks such as the Internet. The programs are recorded on computer readable recording media such as a hard disk, a floppy disk, a CD-ROM, an MO, and a DVD, and are executed such that the programs are read from the recording media by computers.

As has been described above, according to this invention, correctness of an access request on the basis of the patterns of incorrect accesses in an incorrect pattern

database in which the patterns of incorrect accesses to a server are stored and a predetermined estimation rule, and it is decided, on the basis of the estimation result and a predetermined decision rule, whether the access request is given to the server or not, so that it can be decided on the basis of the concrete request contents of the access request without transmission source information of the access request. For this reason, only a correct access request can be given to the server, and the server can be protected from an incorrect access from a client which is not recognized as an incorrect client.

Furthermore, it is estimated that the access request is an incorrect access when the access request corresponds to any one of the patterns of incorrect accesses stored in the incorrect pattern database, and it is estimated that the access request is a correct access when the access request does not correspond to any one the patterns of incorrect accesses stored in the incorrect pattern database, and the decision unit decides that the access request which is estimated as an incorrect access is not given to the server and decides that the access request which is estimated as a correct access is given to the server. For this reason, it can be rapidly and reliably decided, by checking whether the access request corresponds to the pattern of an incorrect request or not, whether the access is an incorrect access

or not. Therefore, the server can be protected from an incorrect access from a client which is recognized as an incorrect client.

Furthermore, a predetermined estimation value is  
5 calculated depending on the degree of correspondence between  
the access request and the patterns of incorrect accesses  
stored in the incorrect pattern database, and the estimation  
value calculated by the estimation unit is compared with  
a predetermined threshold value to decide whether the access  
10 request is given to the server or not. For this reason,  
it can be decided with some margin by comparing the estimation  
value and the threshold value with each other whether the  
access request is an incorrect access or not. Therefore,  
the server can also be protected with some margin from an  
15 incorrect access from the client device which is not  
recognized as an incorrect client.

Furthermore, prior to estimation of correctness, with  
reference to the correction pattern database in which the  
patterns of correct accesses to the server are stored, it  
20 is decided whether an access request corresponds to any one  
of the patterns of correct accesses stored in the correct  
pattern database, and the correctness of only an access  
request which is decided not to correspond to the pattern  
of a correct access is estimated. For this reason, an access  
25 request which corresponds to the pattern of a correct access

is given to the server without being estimated with respect to correctness, and the correctness of only an access request which does not correspond to the pattern of a correct access can be estimated. Therefore, it can be rapidly decided as  
5 a whole whether an access is an incorrect access or not.

Furthermore, on the basis of a predetermined external transmission rule, an access request which is decided not to be given to the server to a predetermined external device. For this reason, information related to an incorrect access  
10 can be rapidly transmitted to an administrator of the server, an administrator of a filtering device, an administrator of an entire server device, an administrator of a public association which monitors the network as a whole, and the like. Therefore, this configuration can urge these  
15 administrators to perform a countermeasure for maintenance of the server.

Furthermore, on the basis of a predetermined storage rule, an access request which is decided not to be given to the server is stored in a predetermined storage unit.  
20 For this reason, information related to incorrect accesses stored in the storage can be analyzed. Therefore, a further countermeasure for maintenance of the server can be performed.

Furthermore, on the basis of a predetermined updating  
25 rule, the incorrect pattern database, the correct pattern

database, the estimation rule, the decision rule, the  
external transmission rule, the storage rule, or an updating  
rule is updated. For this reason, the pattern of an incorrect  
access which is newly found can be registered in the incorrect  
5 pattern database. Therefore, this configuration can  
tactfully cope with incorrect accesses advancing everyday.

Although the invention has been described with respect  
to a specific embodiment for a complete and clear disclosure,  
the appended claims are not to be thus limited but are to  
10 be construed as embodying all modifications and alternative  
constructions that may occur to one skilled in the art which  
fairly fall within the basic teaching herein set forth.